EXHIBIT B

Potter Handy, LLP
Mark Potter, Esq., SBN 166317
Barry Walker, Esq., SBN 195947
Jim Treglio, Esq., SBN 228077
Christina Carson, Esq. SBN 280048
Tehniat Zaman, Esq. SBN 321557
Mail: 100 Pine St., Ste. 1250
San Francisco, CA 94111
(415) 534-1911; (888) 422-5191 fax
Serve@potterhandy.com
Attorneys for Plaintiffs

SUPERIOR COURT OF CALIFORNIA
SANTA CLARA COUNTY

John Diaz, (See additional parties list with plaintiffs attached)

Plaintiff,

v.

23ANDME, INC.,

Defendant.

Case No. 24CV448217

COMPLAINT FOR CIVIL DAMAGES AND INJUNCTIVE RELIEF

1. **Negligence;**
2. **Breach Of Actual and Implied Contract;**
3. **Invasion of Privacy- Intrusion Upon Seclusion;**
4. **Unjust Enrichment.**

JURY TRIAL DEMANDED

COMPLAINT

Plaintiff, John Diaz, (See additional parties list with plaintiffs attached) (collectively "Plaintiffs") allege against Defendant 23andMe, Inc. ("23andMe" or "Defendant") as follows:

SUMMARY:

1. Defendant is a genomic and biotechnology company that looks at an individual's genome for the purpose of creating unique, personalized genetic reports on ancestral

origins, personal genetic health risks, chances of passing on carrier conditions, and pharmacogenetics.[1]

2. To take advantage of Defendant's services, customers had to provide sensitive personal, genetic, and biological information. To gain the trust of potential customers Defendant expressly advertised the importance of security as "Privacy is in our DNA".

3. On or about October 6, 2023, Defendant announced, via their website, that unauthorized threat actors had accessed 23andMe accounts and compiled customer profile information (the "Data Breach").[2]

4. The Data Breach contained millions of individuals' private identifying information (hereinafter "PII"), including, but not limited to: names, sex, date of birth, usernames, genetic ancestry, profile photos, geographical locations, living biological relatives, and data about individuals' ethnicity.

5. Plaintiffs are customers of 23andMe that were victims of the Data Breach. Due to the Data Breach, Plaintiffs' PII was released, stolen, and offered for sale on the dark web.

6. Defendant had a non-delegable duty and responsibility to implement and maintain reasonable security measures to secure, safeguard, and protect the private information that it collected, stored, and maintained for Plaintiffs.

7. Defendant disregarded the rights of Plaintiffs by intentionally, willfully, recklessly, or negligently failing to implement adequate and reasonable measures to ensure that Plaintiffs' PII was safeguarded, failing to take all available steps to prevent unauthorized disclosure of data, and failing to follow applicable, and appropriate protocols, policies, and procedures regarding the encryption of data. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect victims' PII.

8. As a result of Defendant's failure to implement adequate data security measures,

[1] https://www.23andme.com/# (last visited January 9, 2024).
[2] https://blog.23andme.com/articles/addressing-data-security-concerns

Plaintiffs have suffered actual harm in the disclosure of their PII to unknown and unauthorized third parties. Plaintiffs have suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their PII. Plaintiffs also remain vulnerable to future cyberattacks and thefts from the data in Defendant's possession.

9. As such, Plaintiffs assert claims for negligence, breach of implied contract, invasion of privacy, and unjust enrichment.

JURISDICTION AND VENUE:

10. This Court has subject matter jurisdiction over this action pursuant to Article VI, section 10 of the California Constitution and Code of Civil Procedure section 410.10

11. This Court has personal jurisdiction over Defendant because it is headquartered in the State of California, county of Santa Clara, and purposefully avails itself of the laws, protections, and advantages of this State.

12. Venue is proper in this Court because Defendant conducts business in this County and reaped substantial profits from customers in this County. In addition, in its own Terms of Service, Defendant has agreed "…to submit to the exclusive jurisdiction of any state or federal court located in Santa Clara County, California (except for small claims court actions which may be brought in the county where you reside), and waive any jurisdictional, venue, or inconvenient forum objections to such courts." Finally, a substantial part of the acts and conduct charged herein occurred in this County.

PARTIES:

13. Plaintiffs are residents of California who provided 23andMe with a DNA sample for analysis and whose private identifying information was compromised by the Data

Breach.

14. Plaintiff Samantha Canepa is currently a resident of Arizona. Plaintiff Canepa was a resident of California who provided 23andMe with a DNA sample for analysis and whose private identifying information was compromised by the Data Breach as a California resident.

15. Plaintiff Danielle McCulley is currently a resident of Nevada. Plaintiff McCulley was a resident of California who provided 23andMe with a DNA sample for analysis and whose private identifying information was compromised by the Data Breach as a California resident.

16. Defendant 23andMe, Inc. is a biotechnology company headquartered in California that collects and analyzes an individual's genome for the purpose of creating personalized genetic reports directly to consumers.

FACTUAL ALLEGATIONS:

Defendant collected and stored Plaintiffs' PII

17. Defendant collects PII from their customers in the course of doing business.

18. As a condition of receiving Defendant's services, Plaintiffs were required to entrust Defendant with highly sensitive genetic information, information derived from genetic testing, health information, ancestral origin, and other confidential and sensitive PII. 23andMe then stores that information in its platform.

19. According to the Privacy Statement on 23andMe's website, the company collects the following categories of customer information:

a) Registration Information, including name, user ID, password, date of birth, billing address, shipping address, payment information, account authentication information, and contact information (such as email address and phone number).

b) Genetic information, including "[i]nformation regarding your genotype (e.g., the As, Ts, Cs, and Gs at particular locations in your DNA)" and "the 23andMe genetic data and reports provided to you as part of our Services."

c) Sample Information, including "[i]nformation regarding any sample, such as a saliva sample, that you submit for processing to be analyzed to provide you with Genetic Information, laboratory values or other data provided through our Services."

d) Self-Reported Information, including "gender, disease conditions, health related information, traits, ethnicity, family history, or anything else you want to provide to us within our Service(s)."

e) User Content, including "[i]nformation, data, text, software, music, audio, photographs, graphics, video, messages, or other materials, other than Genetic Information and Self-Reported Information, generated by users of 23andMe Services and transmitted, whether publicly or privately, to or through 23andMe. For example, User Content includes comments posted on our Blog or messages you send through our Services."

f) Web-Behavior Information, including "[i]nformation on how you use our Services or about the way your devices use our Services is collected through log files, cookies, web beacons, and similar technologies (e.g., device information, device identifiers, IP address, browser type, location, domains, page views)."

g) Biometric Information, including "[c]ertain Self-Reported Information you provide to us or our service providers to verify your identity using biological characteristics."

20. As part of its advertising, Defendant promises to maintain the confidentiality of Plaintiffs' PII to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiffs' PII for non-essential purposes.

21. Defendant's Privacy Policy states that it "encrypt[s] all sensitive information and conduct[s] regular assessments to identify security vulnerabilities and threats."[3]

22. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' PII, Defendant assumed legal and equitable duties and knew or should have known that it was

[3] https://www.23andme.com/privacy/

responsible for protecting Plaintiffs' PII from unauthorized disclosure.

23. Additionally, Defendant had and continues to have obligations created by applicable state law, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiffs' PII confidential and to protect such PII from unauthorized access.

24. Defendant created the reasonable expectation and mutual understanding with Plaintiffs that it would comply with its obligations to Plaintiffs' information, including the PII, confidential and secure from unauthorized access.

25. Plaintiffs have the utmost privacy interest in the highly sensitive nature of PII and would not have been induced to purchase the genetic testing offered by Defendant had Defendant not included privacy assurances within its advertising.

26. Plaintiffs took reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Data Breach

27. On October 6, 2023, Defendant revealed that threat actors were able to access customer accounts and obtain customers' PII without authorization and consent.

28. Despite the prevalence of public announcements of data breach and data security compromises in recent years, Defendant failed to take sufficient steps to protect Plaintiffs' PII from being compromised.

29. Upon information and belief, Defendant did not require two-factor authentication to protect Plaintiffs' PII at the time of the Data Breach.

30. Upon information and belief, Defendant did not adequately monitor, secure, and/or encrypt its servers and Plaintiffs' PII.

31. Upon information and belief, Defendant could have prevented the Data Breach.

32. Upon information and belief, the cyberattack was expressly designed to gain access

to private and confidential data, including Plaintiffs' PII.

33. Due to Defendant's inadequate security measures, Plaintiffs now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat indefinitely.

Defendant failed to adequately protect the PII and failed to timely notify Plaintiffs their data had been compromised

34. On November 6, 2023, one month after it disclosed the breach, 23andMe announced that it was "requiring all customers use a second step of verification to sign into their account."

35. On information and belief, Defendant did not begin notifying Plaintiffs their specific PII had been compromised until on or after December 1, 2023.

36. On information and belief, Defendant continues to fail to take reasonable and adequate measure to notify all impacted customers that their PII has been compromised.

37. At all relevant times, Defendant had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

38. At all relevant times, Defendant had a duty to properly secure the collected PII, encrypt and maintain such information using industry standard methods, create and implement reasonable data security practices and procedures, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs, and to promptly notify Plaintiffs when Defendant became aware that Plaintiffs' PII may have been compromised.

39. Defendant touted its security and privacy as part of their advertising. Defendant's duty to use reasonable security measures arose as a result of the Plaintiffs' reasonable reliance on Defendant to secure their highly sensitive personal data. Plaintiffs

surrendered the data to obtain Defendant's services under the express condition that Defendant would keep it private and secure. Accordingly, Defendant also has a duty to safeguard their data, independent of any statute.

40. Defendant owed a duty of care to Plaintiffs because they were foreseeable and probable victims of any inadequate data security practices.

Value of the PII

41. PII are highly valuable for identity thieves and personal information is sold on several underground internet websites for $40 to $200[4] per identity.

42. Identity thieves can use PII, such as that of Plaintiffs to perpetrate a variety of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

43. Criminals can also use stolen PII to extort a financial payment by leveraging sensitive healthcare information, for example a sexually transmitted disease or terminal illness, to extort or coerce the victim.

44. Familial relationships and ethnic background can be used to target certain minority groups with threats or even violence.

45. Data breaches involving medical information are more difficult to detect, and take longer to uncover, than normal identity theft. In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief can use private information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[5] The FTC also warns that if a thief's health information is mixed with the victim's it "could affect the

[4] Anita George, DIGITAL TRENDS, Your personal data is for sale on the dark web. Here's how much it costs (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

[5] See What to Know About Medical Identity Theft, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Oct. 2, 2023).

medical care [they are] able to get or the health insurance benefits [they are] able to use."[6]

46. Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiffs. It knew, or should have known, that PII is sought after and valuable target for thieves and that there was a high likelihood this information would be targeted. Therefore, its failure to do so is intentional, willful, reckless, and/or grossly negligent.

47. Defendant disregarded the rights of Plaintiffs by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and/or extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff prompt and accurate notice of the Data Breach.

48. Plaintiffs have suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and suffer fear, stress, anxiety and increased concerns for the loss of their privacy and PII being in the hands of criminals.

49. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

50. As a result of the Data Breach, Plaintiffs are at risk and will continue to be at increased risk of identity theft and fraud for years to come.

51. Plaintiffs have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

[6] *Id.*

Defendant Fails to Comply with FTC Guidelines

52. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

53. FTC guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

54. The guidelines also recommend companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures. Further, it recommends businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[7]

55. The FTC guidelines also form part of the basis of Defendant's duty in this regard.

56. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its customers, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs.

Injuries and Damages:

[7] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting- personal-information.pdf (last visited Oct. 2, 2023).

57. As a result of the Data Breach, Plaintiffs have all sustained actual injuries and damages, including: (i) lost or diminished value of their PII; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) lost time spent on activities remedying harms resulting from the Data Breach; (iv) invasion of privacy; (v) loss of benefit of the bargain; (vi) the continued and certainly increased risk to their PII; and (vii) fear, stress, and anxiety.

58. The information disclosed in this Data Breach is impossible to change. Plaintiffs will have to monitor for identity theft and breaches their entire lives. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Plaintiff. This is a reasonable and necessary cost to monitor to protect Plaintiffs from the risk of identity theft that arose from the Data Breach. This is a future cost that Plaintiffs would not need to bear but for Defendant's failure to safeguard their PII.

CLAIMS FOR RELIEF:

COUNT I: Negligence

(On behalf of all Plaintiffs).

59. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this complaint.

60. At all times herein relevant, Defendant owed Plaintiffs a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Plaintiffs in its computer systems and on its networks.

61. Defendant knew that the PII was private and confidential and should be protected and, thus, Defendant owed a duty of care not to subject Plaintiffs to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

62. Defendant knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate

security.

63. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs' PII.

64. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiffs had entrusted to it.

65. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiffs, Defendant had a duty to adequately protect its data systems and the PII contained therein.

66. Plaintiffs' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions.

67. Moreover, only Defendant had the ability to protect its systems and the PII stored on them from attack.

68. Defendant also had independent duties under state laws that required Defendant to reasonably safeguard Plaintiffs' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant and Plaintiffs.

69. Defendant breached its general duty of care to Plaintiffs in, but not necessarily limited to, the following ways:

a) By failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession;

b) By failing to protect Plaintiffs' PII using reasonable and adequate security procedures and systems that were/are compliant with FTC guidelines and industry-standard practices.

c) By failing to implement processes to detect the Data Breach, security incidents or intrusions,

d) By failing to quickly and to timely act on warnings about data breaches;

e) By failing to timely and promptly notify Plaintiff of any data breach, security incident, or intrusion that affected or may have affected their

PII; and

f) By failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse.

70. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

71. To date, Defendant has not provided sufficient information to Plaintiffs regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs.

72. Further, through its failure to provide clear notification of the Data Breach to Plaintiffs, Defendant prevented Plaintiffs from taking meaningful, proactive steps to secure their PII.

73. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the harm suffered, or risk of imminent harm suffered, by Plaintiffs.

74. Defendant's wrongful actions, inactions, and omissions constituted, and continue to constitute, common law negligence.

75. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs have suffered and will suffer injury, including but not limited to:

a) actual identity theft;

b) the loss of the opportunity of how their PII is used;

c) the compromise, publication, and/or theft of their PII;

d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts

spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft;

f) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' PII in its continued possession; and

g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs.

76. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II: BREACH OF ACTUAL AND IMPLIED CONTRACT
(On behalf of all Plaintiffs)

77. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this complaint.

78. Defendant specifically advertised a feature of the service they offer is privacy and security.

79. Plaintiffs believed their PII would be stored and remain private and secure as a condition of purchasing Defendant's services. In so doing, Plaintiffs entered into actual and implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs if their data had been breached and compromised or stolen.

80. At the time Defendant acquired the PII of Plaintiffs, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

81. Implicit in the agreements between Plaintiffs and Defendant to provide PII, was the Defendant's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) retain the PII only under conditions that kept such information secure and confidential, and (e) provide Plaintiffs with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

82. Plaintiffs fully performed their obligations under the actual and implied contracts with Defendant.

83. Defendant breached the actual and implied contracts they made with Plaintiffs by failing to safeguard and protect their personal information, by failing to delete the information that it no longer needed, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

84. As a direct and proximate result of Defendant's above-described breach of actual and implied contract, Plaintiffs have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse; actual identity theft crimes, fraud, and abuse; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; fear, stress, and anxiety; and other economic and non-economic harm.

85. As a direct and proximate result of Defendant's above-described breach of actual and implied contract, Plaintiffs are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III: INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On behalf of all Plaintiffs)

86. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this complaint.

87. Plaintiffs have a legally protected privacy interest in their PII, which is and was collected, stored and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred with the Data Breach.

88. Plaintiffs reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, removed, and/or disclosed to any unauthorized parties or for any improper purpose.

89. Defendant intentionally intruded into Plaintiffs' seclusion by disclosing without permission their PII to a third party. Defendant's acts and omissions giving rise to the Data Breach were intentional in that the decisions to implement lax security and failure to timely notice Plaintiffs were undertaking willfully and intentionally.

90. By failing to keep Plaintiffs' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiffs' privacy right to seclusion by, inter alia:

a) invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

b) failing to adequately secure their PII from disclosure to unauthorized persons; and

c) enabling the disclosure of their PII without consent.

91. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiffs' PII, leading to the foreseeable unauthorized access, removal, and disclosure of this unguarded and private data.

92. Plaintiffs' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

93. The disclosure of Plaintiffs' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable

person.

94. Defendant's willful and reckless conduct that permitted unauthorized access, removal, and disclosure of Plaintiffs' sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

95. The unauthorized access, removal, and disclosure of Plaintiffs' PII was without their consent, and in violation of various statutes, regulations, and other laws.

96. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiffs suffered injury and sustained actual losses and damages as alleged herein.

97. Plaintiffs alternatively seek an award of nominal damages.

COUNT IV: UNJUST ENRICHMENT

(On behalf of all Plaintiffs)

98. Plaintiffs re-plead and incorporate by reference all prior paragraphs of this complaint.

99. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiffs.

100. Defendant, prior to and at the time Plaintiffs entrusted their PII to Defendant, caused Plaintiffs to reasonably believe that Defendant would keep such PII secure.

101. Defendant was aware, or should have been aware, that reasonable consumers would want their PII secured and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were substandard for that purpose.

102. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiffs' decisions to seek services from Defendant.

103. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiffs made their decisions to make purchases, engage in commerce therewith, and seek services or information.

104. Defendant denied Plaintiffs the ability to make an informed purchasing decision and

took undue advantage of Plaintiffs.

105. Defendant was unjustly enriched at the expense of Plaintiffs, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiffs; however, Plaintiffs did not receive the benefit of their bargain because they paid for services that did not satisfy the purposes for which they bought/sought them.

106. Since Defendant's profits, benefits, and other compensation were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation, or profits it realized from these transactions.

107. Plaintiffs seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits, and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiffs may seek restitution.

PRAYER:

Wherefore, Plaintiffs request that this Court award damages and provide relief as follows:

A. For all compensatory damages, statutory damages, punitive damages, restitution, and/or recovery of such relief as permitted by law in kind and amount;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs;

C. For injunctive relief requested by Plaintiff, including but not limited to:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendant to protect, including through encryption, all data collected through the course of business;

   iii. requiring Defendant to delete and purge the PII of Plaintiffs unless Defendant can provide to the Court reasonable justification for the retention and use of

such information when weighed against the privacy interests of Plaintiffs;

iv. requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' PII;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

vi. prohibiting Defendant from maintaining Plaintiffs' PII on a cloud-based database;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to establish an information security training program for all employees, with additional training for employees' responsible for handling PII;

x. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII;

xi. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

xii. requiring Defendant to meaningfully educate Plaintiffs about the threats they face due to the loss of their confidential PII to third parties, as well as the

steps affected individuals must take to protect themselves;

D. for pre- and post-judgment interest on all amounts awarded, at the prevailing legal rate;

E. for an award of attorney's fees under Civil Code § 56.35, costs, and litigation expenses; and

F. for all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiffs hereby demand a trial by jury for all issues triable by jury.

Dated: September 25, 2024

POTTER HANDY LLP

By: _____

Tehniat Zaman, Esq.
Attorney for Plaintiffs

Potter Handy, LLP
Mark Potter, Esq., SBN 166317
Barry Walker, SBN 195947
Jim Treglio, Esq., SBN 228077
Christina Carson, Esq. SBN 280048
Tehniat Zaman, Esq. SBN 321557
Mail: 100 Pine St., Ste. 1250
San Francisco, CA 94111
(415) 534-1911; (888) 422-5191 fax
Serve@potterhandy.com
Attorneys for Plaintiffs

COMPLAINT: Attachment 1

John Diaz, (See additional parties list with plaintiffs attached) v. 23ANDME, INC.,

1.	Christopher Jermal	CA	28.	Gardell Frost	CA
2.	Justin Ehrman	CA	29.	John Lozano	CA
3.	Alexa Anderson	CA	30.	Angelina Shilling	CA
4.	Tom Causey	CA	31.	Jenai Straker	CA
5.	Kenneth Klein	CA	32.	David Andre	CA
6.	Ravi Yob	CA	33.	Marvin Castaneda	CA
7.	Richard Pham	CA	34.	Haley Halkias	CA
8.	Kimberly Cory	CA	35.	Charan Macias	CA
9.	Cindy Serene	CA	36.	Mark Anderson	CA
10.	Julia Karobkoff	CA	37.	Fern Miro	CA
11.	Miguel Ruiz	CA	38.	Elizabeth Hall	CA
12.	Andrea Huff	CA	39.	Sarah Vaughan	CA
13.	Cambria Nelson	CA	40.	Asia Hunter	CA
14.	Linda Lodge	CA	41.	Dwight Downey	CA
15.	Veronica Avalos	CA	42.	Sean Weaver	CA
16.	Daniel Macias	CA	43.	Edward Lee	CA
17.	Paola Rodriguez	CA	44.	Emi Doncheva	CA
18.	Renee Maese	CA	45.	Nader Halawa	CA
19.	Christopher Sanchez	CA	46.	Deb Hughes	CA
20.	Brad Maeder	CA	47.	Jeanette Rumble	CA
21.	Payton Weide	CA	48.	Monica Paredes	CA
22.	Tracy Burgos	CA	49.	Steve Nosanchuk	CA
23.	Alan Alvarez	CA	50.	Bailey Sillas	CA
24.	Katie Paige	CA	51.	Sally Ornelas	CA
25.	Joseph Montes	CA	52.	Shauna Sharpless	CA
26.	Joshua Brock	CA	53.	Gloria Lopez	CA
27.	John Lorenz	CA	54.	Michael Gillaspy	CA

55.	Lorena Torres	CA
56.	Adam Seal	CA
57.	Izadora Lima	CA
58.	Ocean Jarwin	CA
59.	John Metivier	CA
60.	Marc Kenney	CA
61.	Teresa Silveira	CA
62.	Heike Althaus	CA
63.	Cassandra Cummings	CA
64.	Susan Salop	CA
65.	Rosita Cortez	CA
66.	Derek McDow	CA
67.	Meredith Gardner	CA
68.	Iker Franco	CA
69.	Joseph Dovidio	CA
70.	Carlos Strunk	CA
71.	Etta Thordarson	CA
72.	Elizabeth Bernal	CA
73.	David Arriola	CA
74.	Jon Directo	CA
75.	Ceaser Flores	CA
76.	Mushun Richardson	CA
77.	Frederick Frazier	CA
78.	Mary-DeLaney Bukosky	CA
79.	Michael Crosbie	CA
80.	Francisco Jimenez	CA
81.	M Ollis	CA
82.	Johnetta Pianosi	CA
83.	David Powell	CA
84.	Daisy Cordova	CA
85.	Sabrina Mena	CA
86.	Karl Ward	CA
87.	Cassandra Solano	CA
88.	Jasmine Snowden	CA
89.	Erin Parks	CA
90.	Farshad Tehrani	CA
91.	Samantha Canepa	AZ
92.	Brenda Igig	CA
93.	Sharan Harvey	CA
94.	Roxanne Rosales	CA
95.	Hayley Atkins	CA
96.	Cynthia McCormick	CA
97.	Amber Lacour	CA
98.	Ofelia Gomez	CA
99.	Alexis Gutierrez	CA
100.	Jill Williams	CA
101.	Joseph Carlin	CA
102.	Shari Hartwell	CA
103.	Daniel Alvadroza	CA
104.	Alexandra Hurtado	CA
105.	Joshua Thorburn	CA
106.	Barry Hickson	CA
107.	Shreya Badhrinarayanan	CA
108.	Patrick Peterson	CA
109.	Rebecca Lieberman	CA
110.	Amanda Stahmer	CA
111.	Renata Martin Pedroza	CA
112.	Anton Doty	CA
113.	Danielle McCulley	NV
114.	Jessie Hewitt	CA
115.	Nancy Willard	CA
116.	Dana Ellsworth	CA
117.	Alea Sanders	CA